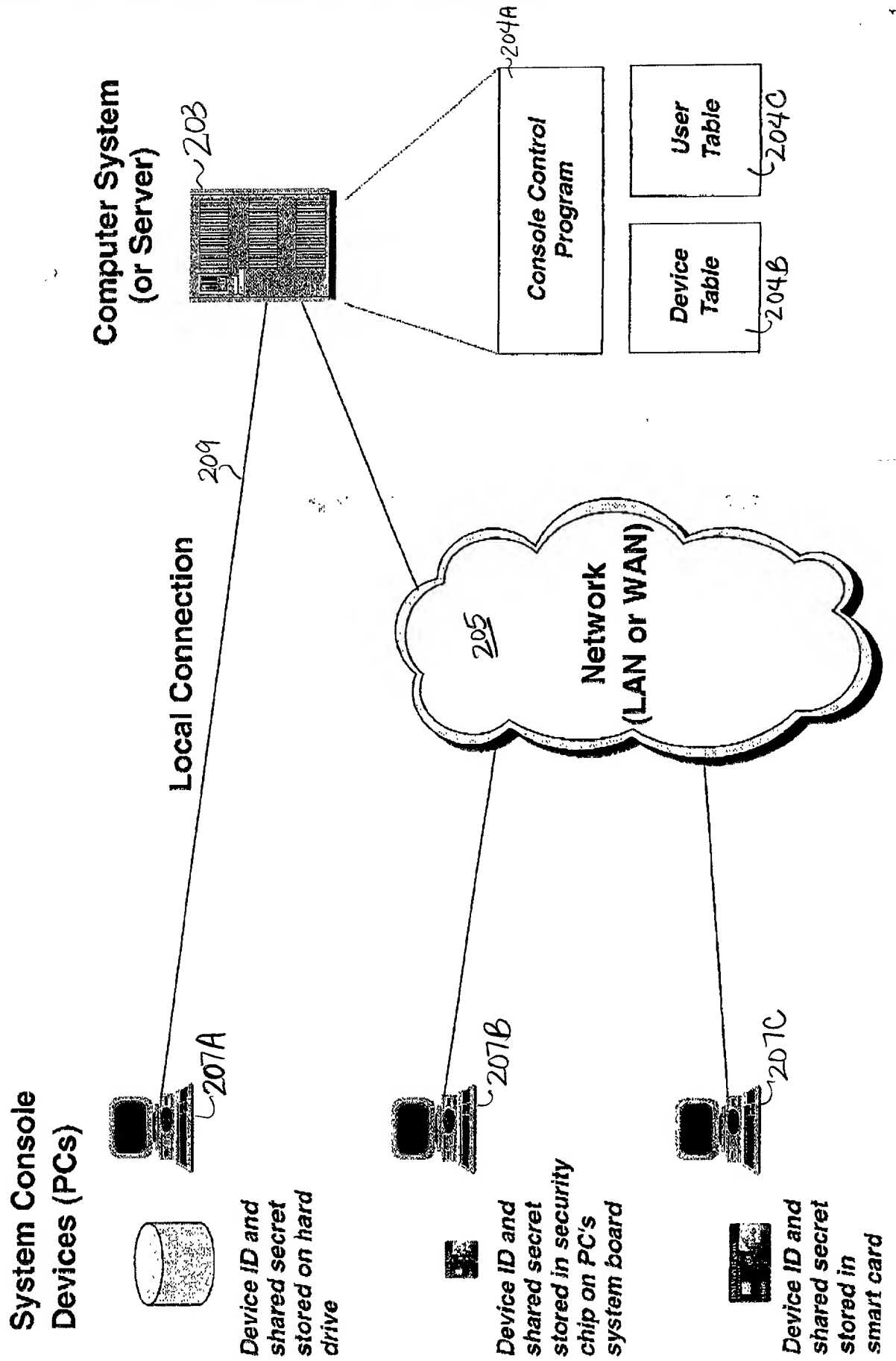


Fig. 1

FIG. 20



321

Op Console PC

OS/400

Console session flow

Normal flow -

prompt for I_b , P_A , I_{ux} , P_{ux}

Setup wizard -

1) prompt for I_b , P_D , P_A , I_{ux} , P_{ux}

2) use PKCS-5 to encrypt P_D with P_A

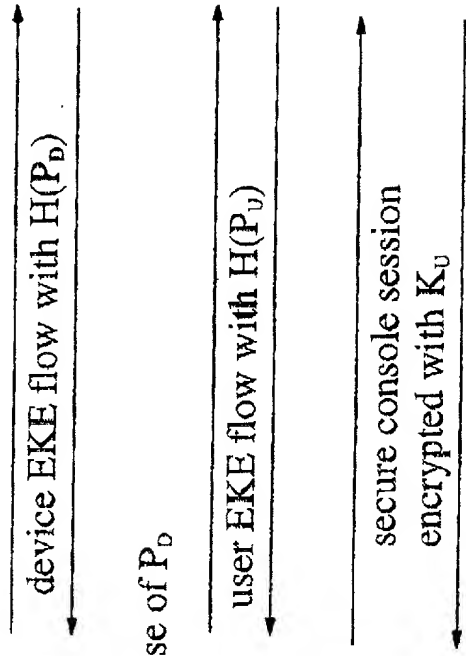
Shipped with:

$I_b = QCONSOLE, H(P_D) = H(QCONSOLE)$

$I_{ux} = QSECOFR, H(P_{ux}) = H(QSECOFR)$

$I_{b2} = 22222222, H(P_{ux}) = H(22222222)$

$I_{u1} = 11111111, H(P_{u1}) = H(11111111)$



Legend:

- I_b = Device identifier
- P_D = Device shared secret
- P_A = Access passphrase
- I_{ux} = User ID
- P_{ux} = User passphrase
- K_D = Device session key
- K_U = User session key

$K = \text{Random number}$
 $H(x) = \text{Hash of } x$

NOTE: The first console session uses the well known shipped device identifier and user ID to access the iSeries. The device passphrase is modified in the initial flow ($P_D = K_D$). Therefore, the genesis device essentially "gets in free."

- generate DH parameters g and p
- where g = base; p = prime; these values do not have to be secret ($public - info$)
- make g and p constants in server and client EKE code

client EKE

make g, p constants

generate R and do DH Phase 1

send -->

device ID, $H(P_D)[public-info]$

server EKE

make g, p constants

generate R and do DH Phase 1

generate challenge B

derive K from DH Phase 2

<-- send (Phase 1 public-info)

$H(P_D)[public info], K[challenge B]$

derive K from DH Phase 2

generate challenge A

send -->

$K[challenge A, challenge B]$

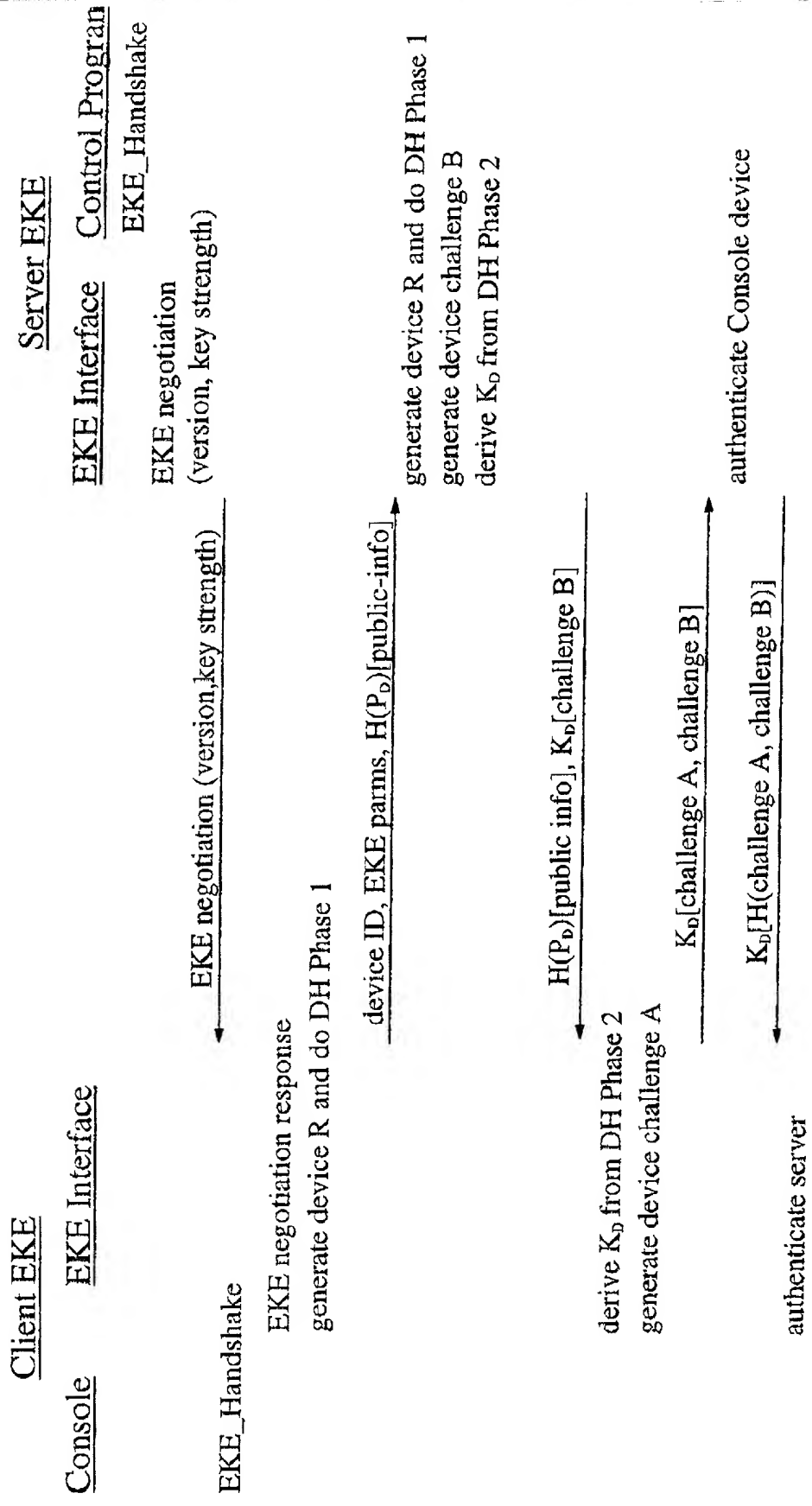
authenticate user A

<-- send $K[H(challenge A, challenge B)]$

authenticate server B

Refer to BSAFE Reference Manual for description of DH Phase 1 & 2.

NOTE: The challenge strings must be a different length than the encryption block.



Pass 1 for device complete,
begin Pass 2 for user...

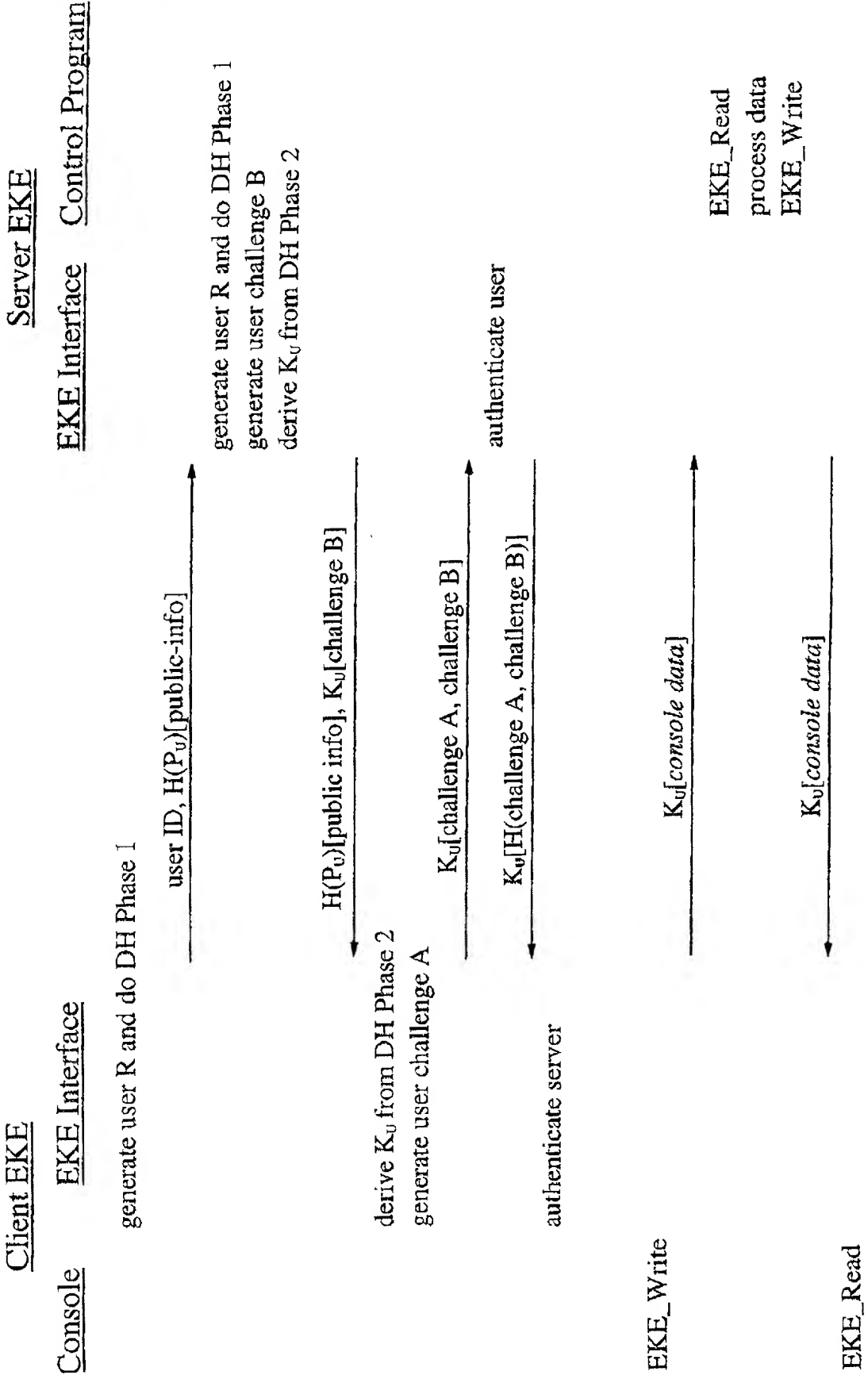


FIG 4A

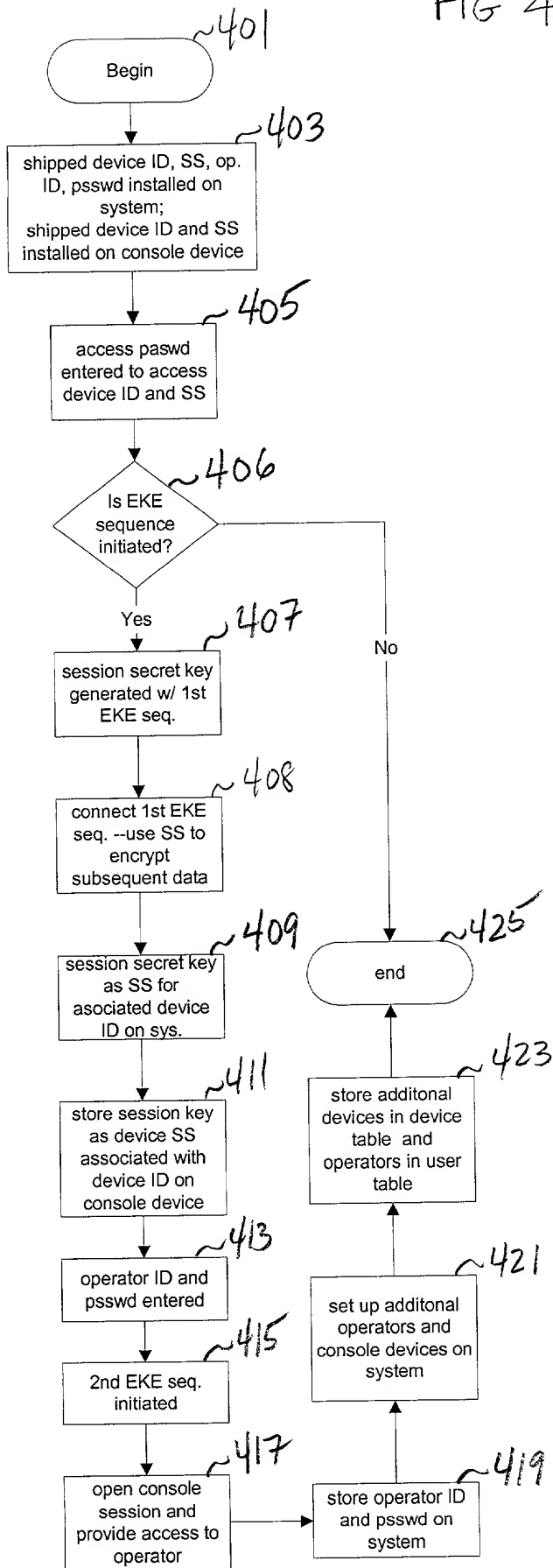


FIG. 4B

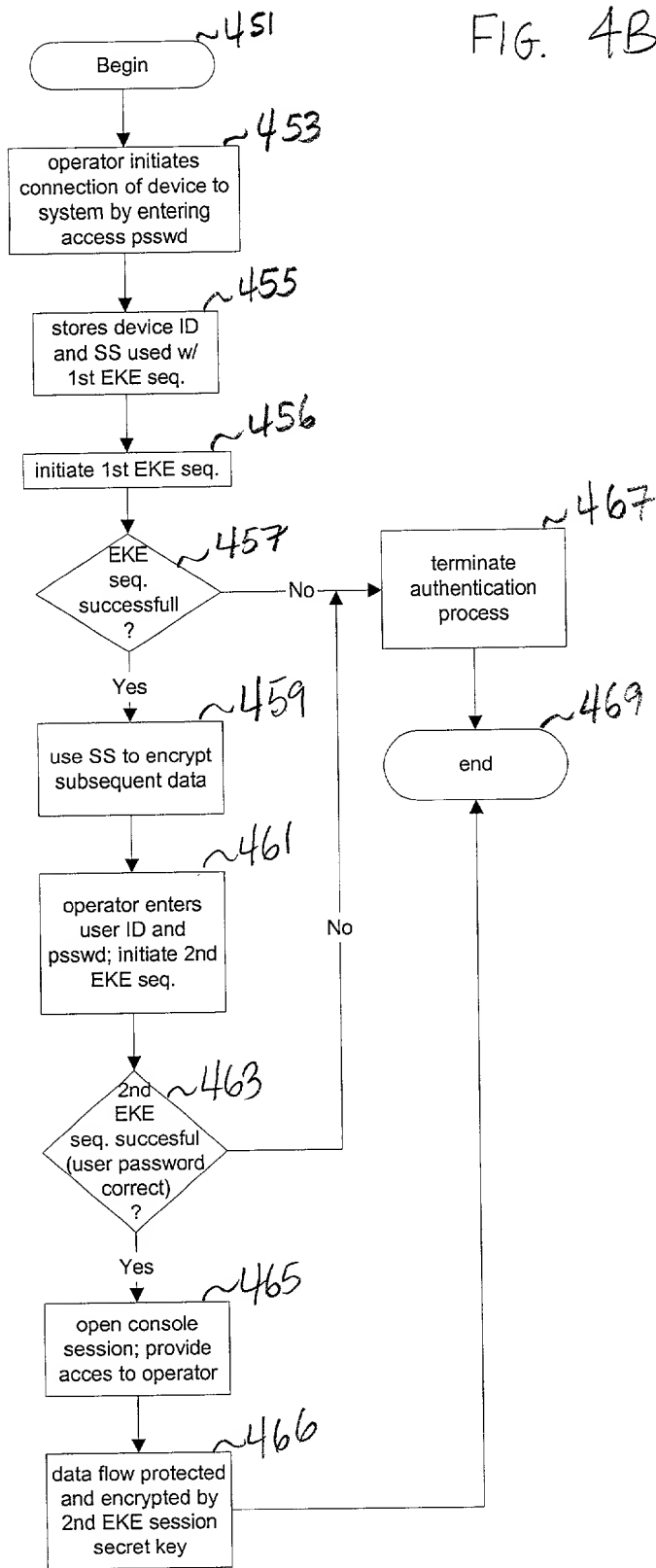


FIG 5A

Client Device (PC) 501

Server Connection	
Server1	Hash (device identifier, shared secret)
Server2	Hash (device identifier, shared secret)

Server

Device Table

Device Identifier	Hashed shared secret
QCONSOLE	H(shared secret)
DEVICE2	H(shared secret)

User Table

User Identifier	Hashed password
11111111	H(password)
22222222	H(password)
QSRV	H(password)
QSECOFR	H(password)